

ABSTRACT OF THE INVENTION

A method and device for protecting a network by
5 monitoring both incoming and outgoing data traffic on multiple
ports of the network, and preventing transmission of
unauthorized data across the ports. The monitoring system is
provided in an non-promiscuous mode and automatically denies
access to data packets from a specific source based upon an
10 associated rules table. All other packets from sources not
violating the rules are allowed to use the same port. The
monitoring system processes copies of the data packets
resulting in minimal loss of throughput. The system is also
highly adaptable and provides for dynamic writing and issuing
15 of firewall rules by updating the rules table. Information
regarding the data packets is captured sorted and cataloged to
determine attack profiles and unauthorized data packets.